International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 10, Number 1 (2018), pp. 11-34

http://www.irphouse.com

Cybersecurity in WebGIS Environment

Giribabu D*
Scientist, Regional Remote Sensing Centre – West, NRSC/ISRO, Dept of Space, Jodhpur, India.

Kamal Pandey
Scientist, Indian Institute of Remote Sensing, Dehradun, India.

Dr. Rao K.R.M
Scientist, National Remote Sensing Centre - Hyderabad, India.

Dr. Srinivasa Rao S
Scientist & General Manager Regional Remote Sensing Centre – West, NRSC/ISRO, Dept of Space, Jodhpur, India

Dr. Udayraj
Scientist & Chief General Manager, National Remote Sensing Centre - Hyderabad, India.

Vinod M Bothale
Scientist & Group Director, National Remote Sensing Centre - Hyderabad, India.

Dr. Sudhakar Reddy C
Scientist, National Remote Sensing Centre - Hyderabad, India.

Dr. Prasada Rao P.V.V
Professor, Andhra University, Vishakhapatnam, India.

Dr. Santanu Chowdhury
Scientist & Director, National Remote Sensing Centre - Hyderabad, India.

Corresponding author

Abstract

Cybersecurity is a global challenge as Cyberspace is never risk free. Cybersecurity ensures the attainment and maintenance of the security properties of the digital infrastructure and services against relevant security risks in the cyber environment. Currently web applications are highly functional and rely upon two-way flow of information between the server and browser. New technologies in Web applications have brought with them a new range of security vulnerabilities and new possibilities for exploitation. WebGIS is an effective way for disseminating geospatial data and geo-processing tools through internet. WebGIS is similar to the client/server architecture and the server-side geo-processing components will store, process and serve the data to the client/browser, during which Database server, Application server and a web server will be involved. The networking infrastructure in WebGIS environment plays a critical role in the security of the data centres. This paper presents the architecture of WebGIS environment, role of networking components, traits of Cybersecurity and portrays various defence mechanisms that aid in Cybersecurity in WebGIS environment

Keywords: Cybersecurity, GIS, WebGIS, Vulnerabilities, OWASP, ENISA Threat Landscape

I. INTRODUCTION

Cybersecurity is a global challenge as Cyberspace is never risk free. Cybersecurity ensures the attainment and maintenance of the security properties of the digital infrastructure and services against relevant security risks in the cyber environment. von Solms, R and van Niekerk, J in their article conveyed that the boundaries of Cybersecurity as a concept are wider than those of information security in terms of how it is formally defined. It is outlined that the Cybersecurity is a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment of organization and user's assets [1].

In spatial sciences, technological advances have led to a tendency for geographic data to be digital, and computer mapping is now standard [2]. Spatial data are data which represent objects that have physical dimensions – they take up space [3]. A Geographic Information System (GIS) is a system designed to capture, store, manipulate, analyze, manage, and present spatial data. Burrough defines GIS as "a powerful set of tools for collecting, storing, retrieving at will, transforming, and displaying spatial data from the real world...."[4]. Internet technology reduces the cost of data management and information distribution to mass usages, thus web based information systems are evolving mostly as applications throughout the world [5]. Internet based GIS or WebGIS is one area which evolved as a very useful online service due to rapid development of web technology and GIS [6]. WebGIS platform

made geographic information accessible to everyone and it has broadened its reach significantly by abstracting geographic data into standard spatial services like travel Apps, disaster & emergency services, tourism, natural resource management and etc. Agrawal, S & Gupta R.D mentioned about evolution of WebGIS and described about its major events of development [7].

Network infrastructure is the hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network. It provides the communication path and services between users, processes, applications, services and external networks or the internet.

This paper presents the architecture of WebGIS environment and presents various defence mechanisms that aid in Cybersecurity of WebGIS environment. The paper is organized as follows. Section 2 describes architecture and data flow in WebGIS setup. In Section 3 the networking components of server side infrastructure on the lines of OSI layer as model has been illustrated. Section 4 gives glimpses of Cybersecurity concepts. Section 5 articulates the implementation of Cybersecurity in WebGIS environment and finally section 6 gives the conclusion.

II. ARCHITECTURE AND DATA FLOW IN WEBGIS SETUP

In general terms the anatomy of data flow between client and web server in Internet starts from a request from client's web browser, script or tool to a web server which hosts the web site containing html documents, images, videos, stylesheets, JavaScript files and etc. Certain events will happen during this process like querying the Domain Name Server (DNS) to find the IP address of the web server, later Open System Interconnection (OSI) model will ensure the standard of communication between the client and Web server. The requests will reach web servers after passing through firewalls and/or load balancers. The entire communication between client and server takes place using the Hypertext Transfer Protocol (HTTP) [8]. Leading Web servers include Apache, Microsoft's Internet Information Server (IIS) and nginx (pronounced engine X) from NGNIX, Novell's NetWare server, Google Web Server (GWS) and Domino servers from IBM [9].

More often Web servers will deliver the requests in the form of HTML documents, which may include compressed images, style sheets and scripts in addition to the text content. Web applications dealing with non-spatial data may contain only Web servers, but WebGIS platform intends to serve Georeference data (i.e., each cell or feature contains information about its position on Earth) which will be in the form of raster (like GeoTiff format) or vector (like shapefile format). But browsers are not capable to display Georeferenced data instead they are developed to display compressed formats like PNG, JPG or GIF which cannot store the geocoded information. The compressed images which are smaller in size often travel faster and became norm of image display in client side browsers.

Hence there is a requirement for another server with a GIS engine which will take input in the form of Georeferenced data and converts into compressed formats like

PNG, JPG or GIF. Certain times the output can be of XML based like yielding as a vector format (e.g. KML, GML). To do mapping activity commercial of the shelf (COTS) software like ArcGIS server and free and open source software (FOSS) like GeoServer, MapServer, Mapnik, QGIS server, MapGuide are available [10]. Usually the GIS engine is installed in application server which will exposes certain services. Open Geospatial Consortium (OGC) defined a set of standards for distributing geographic data and make layers of information more accessible. As defined by OGC, the web mapping service consists of two functions: (i) Get-Capablites that defines the capabilities of a server such as defining the supported file formats, the available map layers, and the method of display; and (ii) GetMap that tells the database what is needed. The database reads a request and creates the map-based data from the requirements that have been defined by GetCapabilities. The requested data package is then sent to the web mapping service [10]. The OGC standard has led to the development of services like below [11].

- Web map service (WMS) – georeferenced map images typically in the form of raster tiles (PNG, GIF, or JPG). The tiles can also be delivered in a vector format. Requests are made using a standard web URL address.
- Web coverage service (WCS) – a geographical area that can be overlaid upon a map but cannot be edited or analyzed. WCS is used to transfer coverages that consist of objects such as data points, pixels, or paths defined with vectors.
- Web feature service (WFS) – allows requests for geographical features, essentially providing the information behind the map. WFS allow features to be queried, updated, created, or deleted by the client. This data is usually provided in an XML format like KML or GML.

GIS Engine like GeoServer reads geographic data from a variety of database and non-database formats like PostgreSQL, Oracle Spatial, GeoTiff, Shapefile and etc. A separate Database Server ensures optimized serving of data to the GIS Engines [11]. Non spatial data is usually stored in relational database and usually provides Structured Query Language (SQL) to query, manipulate and extract data. Databases like PostgreSQL will support spatial functionalities with extensions like PostGIS. The geometry extension like PostGIS enables the support all the type of features viz., point, line and polygon. Spatial database is a very important part of the Web-GIS architecture and it allows the storage and querying of data that is related to objects in space, represented either in vector or raster forms [12].

Figure 1 shows typical architecture of a WebGIS setup. WebGIS implementation is predominantly a Client/Server model. In 'thin client' approach, most of the processing is done at the server side after a simple request from the client. And in 'thick client' approach the client is more powerful by augmenting its capabilities with the help of plug-ins, applets or some additional modules. More recently, hybrid approaches have been explored to balance the merits and demerits of these thin client and thick client approach [13, 14, 7]. More information on the architecture details and components of WebGIS environment can be inferred from the studies made by [15, 16, 17, 18, 19, 20, and 21].

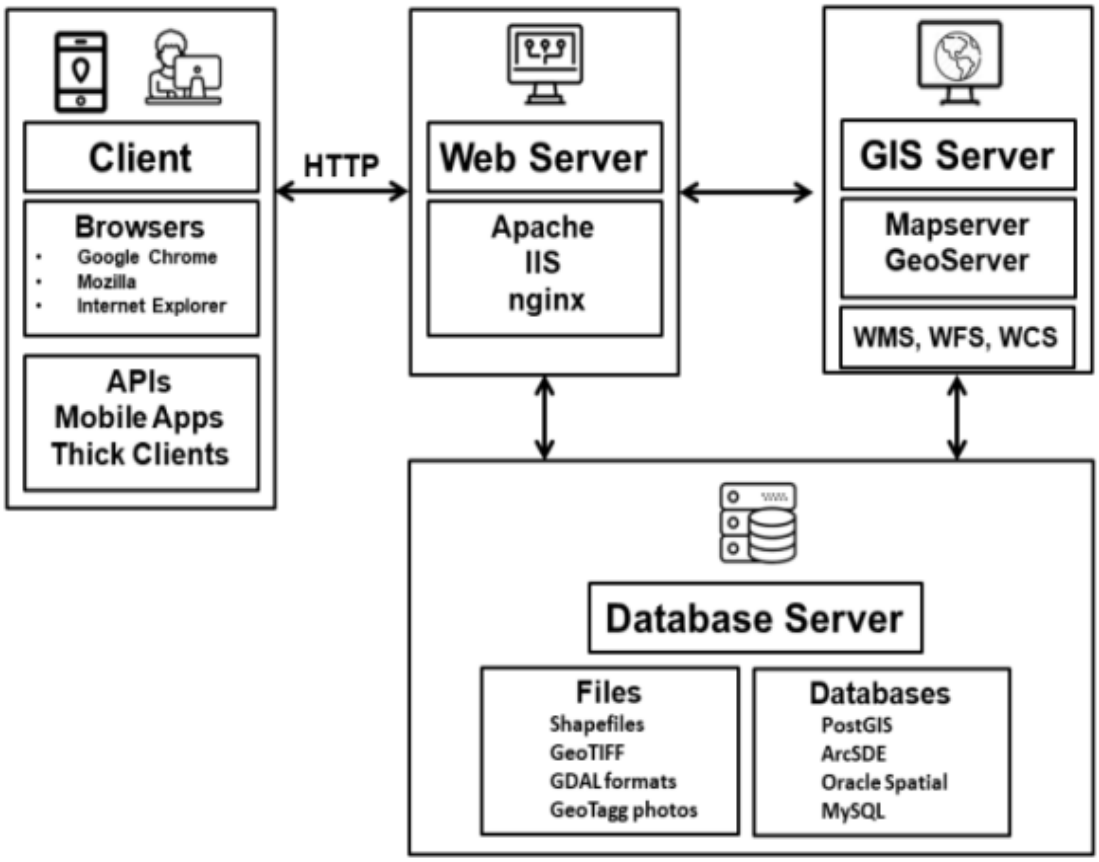

Figure 1. Typical Architecture of WebGIS Environment

III. NETWORKING COMPONENTS OF SERVER SIDE INFRASTRUCTURE

Server side infrastructure contains various resources in well controlled environments and under central management, which enables services around the clock or according to the strategic needs. These computing resources include web servers, application servers, file and print servers; mail servers, application software and the operating systems that run them, storage subsystems; and the network infrastructure [22]. OSI layers are a reference model for how applications communicate over a network. The main concept of OSI is that the process of communication between two endpoints in a network can be divided into seven distinct groups of related functions, or layers. Each communicating user or program is on a device that can provide those seven layers of function [23]. Table I adopted from [24] illustrates the layer functioning with examples of medium. Transmission Control Protocol (TCP) and Internet Protocol (IP) are two distinct computer network protocols mostly used together. Due to their popularity and wide adoption, they are built in all operating systems of networked devices.

Table I. OSI layers and their functioning

Layer No.	OSI Layer	Layer Function	Units	Example of Medium	TCP/IP Model
1	Physical	Physical	Binary digits	Cat 6 cable, SX fiber	Network
2	Data Link	Data link	Ethernet frames	Ethernet switches, hubs	
3	Network	Network	IP addresses	Routers	Internet
4	Transport	Transport	TCP, UDP, ICMP	TCP port 80 for HTTP, UDP port 161 for SNMP	Transport
5	Session	Session, presentation and application	URL, cookie	http://www.url.com or cookies	Application
6	Presentation				
7	Application				

Essentially a data centre contains the layer 2 (data link) and layer 3 (network) devices like below.

- Switches and Routers
- Firewalls
- Intrusion detection and prevention systems
- Load balancers
- Reverse proxies
- SSL (Secure socket layer) offloaders
- Caches.

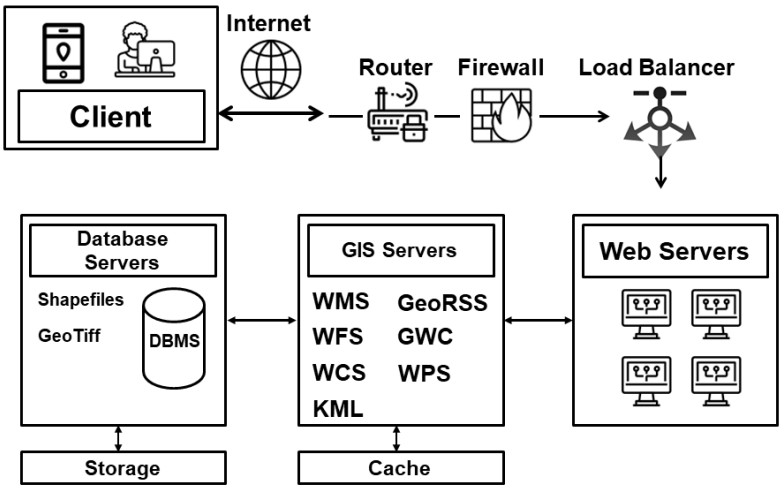

Figure 2. Networking Components in WebGIS Environment

Figure 2 shows the lineage of networking compoinents in WebGIS envionrment. The network infrastructure plays a critical role in the security of the data centres. In most configurations, the network infrastructure will be the first line of defence between a public Web server and the Internet [25]. From [26] the description of these networking elements is as follows.

- Switches are network devices that move network packets (unit of data that is routed between an origin and a destination on the Internet) from one device to another at OSI layer 2. Switches can determine MAC addresses of the packets destination devices by monitoring network traffic. Once destination addresses are determined, switches can send specific packets to the port that connects to the network adapter with a specific MAC address.
- Routing devices are capable to exchange information with other routers on the network to determine the most efficient path from one device to another. (However enterprise-level switches could have the capability to route packets at OSI layer 3 between network segments, and thus could be used as routers).
- Firewall is a network device that controls the flow of traffic between network segments using OSI layer 3 addresses in order to meet security requirements. Firewall services could be implemented by a dedicated hardware device (particularly to protect the boundary between the internal network and the Internet), or by a network host running software firewall.
- An Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Some IDS have the ability to respond to intrusions. Systems with response capabilities are typically referred to as an Intrusion Prevention System (IPS).
- Load balancer is a network device that facilitates horizontal clustering, where multiple servers are configured to perform the same function on the network. The load balancing functionality may be provided by software or a hardware device.
- Reverse proxy is a type of proxy server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client as if they originated from the Web server itself.
- Secure socket layer (SSL) certificates provide authentication between a server and a client computer in a Web application. SSL offloading takes all the processing of SSL encryption and decryption off the main Web server and moves it to a separate device designed specifically for the task. This allows the performance of the main Web server to increase and it handles the SSL certificate efficiently.
- A cache stores frequently accessed Web content to improve response time and save network bandwidth.

The main goal of any data centres should ensure the characteristics like scalability, availability, manageability, security, quality of service [22]. However the characteristics like scalability, availability, manageability and quality of service depends on the organisational management practices. But one cannot compromise with the security of the data centre and it should be managed by best practises and by

an active bodies or committees with experts.

Once the Web server has been positioned in the network, the network infrastructure elements should be configured to support and protect it. But at the same time these network elements alone cannot provide complete web security. The frequency, sophistication, and variety of attacks perpetrated today lend support to the idea that web security must be implemented through layered and diverse protection mechanisms called defence-in-depth [25].

IV. CONCEPTS OF CYBERSECURITY

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise availability, integrity (including authenticity and nonrepudiation) and confidentiality. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) mandate is to develop, maintain and promote standards in the fields of information technology (IT) and Information and Communications Technology (ICT). The international standards as per ISO/IEC 27032, 2012 addresses "Cybersecurity" or "Cyberspace security", defined as the "preservation of confidentiality, integrity and availability of information in the Cyberspace". In turn "the Cyberspace" is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".

Surman, Reed, and Meghanathan explained the security components at different OSI layers [27, 28, and 29]. Reed summarized Vulnerabilities and controls measures with respect to all the levels of layers [28].

The Physical Layer is at the bottom of the OSI stack is where the data moves in the form of zeroes and ones, and the actual transmission of data between devices occurs. All layers above depend upon the physical layer to deliver the data. One common operational risk in this area is the disruption of power supply to the network. Another component of the physical layer that is widely used in organizations is the wireless Ethernet or WiFi. A disruption in WiFi signal can cripple the operations of business activities of a company [30].

The Data Link layer of the OSI Model is responsible to place frames on the network medium and ensure that delivery is error free. This media layer involves all the data packets which are moved by the physical layer. A defining protocol of this layer is the Address Resolution Protocol (ARP). Every computer with a network interface card (NIC) has a unique media access control (MAC) address. ARP allows one computer, a source, to ask other computers for the MAC address it wants to communicate with. A significant risk at this layer is called ARP Cache Poisoning. Efforts to bypass virtual Local Area Network (VLAN) security protocols and the spoofing of network interface identifying media access control or MAC addresses are typical vulnerabilities of this layer, and successful exploits can go on to compromise the

security of the network layer. Filtering MAC addresses and ensuring that all wireless applications have authentication and encryption built in are common security strategies for this layer [31].

The Network layer is concerned with the global topology of the internet work and is used to determine what path a packet would need to take to reach a final destination over multiple possible data links and paths over numerous intermediate hosts. Routers and firewalls operate at this layer. It is at this layer that best path is determined from source to destination host on a network. This layer is the last layer that has a rough physical correspondence to the real world. Defence through obscurity augments a comprehensive solution at this layer. Network Address Translation (NAT) is a service that temporarily assigns a private IP address to a public IP address. In this sense, for a time, there is a one-to-one relationship between a private and a public address. It is necessary to lease a pool of public IP address for NAT to work. Port Address Translations (PAT), on the other hand, allows a single public IP address to be bound to multiple virtual ports. In this way, multiple networked hosts can share a single public identity on the Internet, providing a more cost effective and secure solution. In either event, the internal IP address is hidden to the outside world, providing with some anonymity [32].

The Transport layer ensures the reliable arrival of messages and provides error checking mechanisms and data flow controls. The Transport layer provides services for both "connection-mode" transmissions and for "connectionless-mode" transmissions [27]. Locating a system on the Internet requires knowledge of public IP address assigned to it. An intruder would need to know the IP address to locate the system and the port number assigned to the application, collectively referred to as a socket. A computer system has 65535 ports. These ports can be further broken down into three categories: well known, registered and dynamic. This is where Layer 4 security is applied. Transport control protocol (TCP) allows data to be transported reliably and with error checking. Essential TCP was designed to get data from point A to point B and ensure it was in the same condition as when it left the source. Many applications utilize well known TCP and UDP ports. Trojans, malicious programs masquerading as benign programs, tend to target specific TCP and UDP ports. An open port that is infected by a Trojan will require cleaning. Virus scan software helps to protect systems at this layer.

The Session Layer is concerned with the organization of data communications into logical flows. It takes the higher layer requests to send data and organizes the initiation and cessation of communication with the far end host. The session layer then presents its data flows to the transport layer below where actual transmission begins. Session protocols will often deal with issues of access and accessibility, allowing local applications to identify and connect to remote services, and advertising services to remote clients and dealing with subsequent requests to connect. The session layer also deals with higher-order flow control from an application perspective; just as the transport layer may control transmission from a network-oriented perspective and limit the flow to match the available network capacity, the session layer may control the flow up through to the application layer and limit the

rate that data enters or leaves that realm based on arbitrary or dynamic limits [28]. In the Session Layer, identity is the key factor, and the main controls at this layer focus on the establishment of identity. Secure channels of user and session authentication are essential to private communications. Cryptography technology allows for both the reliable identification of remote parties and the means for protecting the exchange of data from prying eyes. Passwords and other user credentials should be passed and stored in encrypted form to prevent interception or theft. User accounts should have expiration dates based on both usage and fixed time, requiring the update of credentials and reauthorization of access. Session identification may need to be based on a cryptography technology in order to protect sensitive communications in real-time environments.

Presentation layer ensures the data that comes from the source is able to be read by the recipient. A presentation layer program would break down the data to binary so it can travel down and back up the layers and then be reconstructed at the other end of the presentation layer so it can be read by the recipient. The presentation layer essentially ensures that the data is acceptable by both the application and session layers. This layer allows for the standardization of data and the communication of data between dissimilar hosts, such as platforms with different binary number representation schemes or character sets (ASCII vs. UNICODE, for example.) Presentation Layer protocols typically rely upon a standardized data format for use on the network, and various conversion schemes to convert from the standardized format into and out of specific local formats. The Presentation Layer can also control network-layer enhancements such as compression or encryption. Vulnerabilities at this layer often originate from weaknesses or shortcomings in the implementation of the presentation layer functions.

The Application layer deals with the high-level functions of programs that may utilize the network. User interface and primary function live at this layer. All functions not pertaining directly to network operation occur at this layer. Malware protection should be pervasive at layer seven of the OSI Model. Viruses, Worms and Trojans are well known type of malware. Viruses are malicious code attached to a host of file of sorts. This could be application, document or executable file types. Worms are also malicious code that spread from system to system replicating malicious program that are embedded into seemingly functional programs that a user would intentionally download and install. Spyware is another form of malware wreaking havoc on the Internet. Spyware is software that runs on a computer and reports user behaviour and system information back to a source location. Adware is software that enables the posting of banners and advertisements on the host computer. The Open Web Application Security Project (OWASP) is a not-for-profit group that helps organizations develop, purchase, and maintain software applications that can be trusted. OWASP seeks to educate developers, designers, architects and business owners about the risks associated with the most common Web application security vulnerabilities. The organization publishes a popular top ten list that explains the most dangerous Web application security flaws and provides recommendations for dealing with those flaws [33] Table II depicts the top ten most critical web applications security risks for the year 2017.

Table II. OWASP Top 10 - 2017.

Sl. No.	Vulnerability Name	Description
1	Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2	Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
3	Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data. Attackers may steal or modify such weakly protected data to conduct mal-practice. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
4	XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
5	Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc
6	Security Misconfigur ation	This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

Sl. No.	Vulnerability Name	Description
7	Cross Site Scripting (XSS)	XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
8	Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
9	Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.
10	Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.

The OWASP Top 10 Vulnerabilities list is designed to help security professionals and developers to figure out where to start in the application security practice. Every organisation may have similar technology to figure out the trending vulnerabilities and accordingly strategies can be laid out. There are many risk assessment models for the web application risk modelling like OWASP, CENZIC, CVSS, DREAD, OCTAVE, NIST, NISA, ISO 1799 or 27001 for addressing the risk they are dealing with [34]. All these models based on a uniform algorithm and quantify the risk of the application in its own metric.

Cybersecurity is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace. Cyber security consists of a continuing cycle of structured actions to:

- Identify (understand state and risks to systems, assets, data, and capabilities)
- Protect (implement the appropriate safeguards)
- Detect (implement ability to identify a Cybersecurity event)
- Respond (implement ability to take action following a Cybersecurity event)
- Recover (implement resilience and restoration of impaired capabilities)

All of the above activities rely on the trusted, timely sharing of related structured information [35]. To address these structured actions there exists a Cybersecurity ecosystem containing organisation or groups like Advanced Cyber Defence Centre (ACDC), European Network and Information Security Agency (ENISA), European

Telecommunication Standards Institute (ETSI), National Institute of Standards and Technology (NIST) and so on. Beyond this each and every country may have a governing body for ensuring Cybersecurity. The main agenda of this cyber security ecosystem is to develop techniques, technical standards, frameworks and operational practices, maintaining forums, information exchange and mitigation standards.

The ENISA Threat Landscape (ETL) provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends. ETL consists of a list with top threats prioritized according to the frequency of appearance and not according to the impact caused. This report appears on a yearly basis [35]. Table III depicts the top 15 cyber-threats of the year 2017.

Table III. ENISA Threat Landscape 2017

Sl. No.	Top Threats 2017	Description
1	Malware	Malware or malicious software which is specifically designed to disrupt, damage, or gain authorized access to a computer systems.
2	Web based attacks	Web based attacks are those that make use of web-enabled systems and services such as browsers, websites, and the IT-components of web services and web applications. Examples of such attacks include web browser exploits, web servers and web services exploits, drive-by attacks, waterholing attacks, redirection and man-in-the-browser-attacks
3	Web application attacks	Web application attacks are those attacks directed against available web applications, web services, and mobile apps. Such attacks try to abuse APIs that are incorporated in web applications.
4	Phishing	Phishing is a quite pervasive attack because it primarily uses social engineering to attack end users. Phishing is an important infection vector for all types of threat agents. Phishing is highly used as the first step in cyber-attacks and is the most successful infection vector for data breaches and security incidents in both targeted and opportunistic attack tactics.
5	Spam	Spam is one of the most prevalent and persistent cyber-threats.
6	Denial of service	Denial-of-Service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a system resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Sl. No.	Top Threats 2017	Description
7	Ransomware	Ransomware is a form of malicious software (or malware) that, once it's taken over user's computer, threatens with harm, usually by denying the access to data. The attacker demands a ransom from the victim.
8	Botnets	A botnet is a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware. Users are often unaware of a botnet infecting their system.
9	Insider threat	Insider threat refers to the threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of an organisation.
10	Physical manipulation/damage/theft/loss	Though not always a technical/cyber threat, physical manipulation/damage/theft/loss continues to have severe impact on all kinds of digital assets
11	Data breaches	A data breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion.
12	Identity theft	Identity theft is a cyberthreat in which the attacker aims at obtaining confidential information that is used to identify a person or even a computer system. Such confidential information may be: identifiable names, addresses, contact data, credentials, financial data, health data, logs, etc. Subsequently, this information is abused to impersonate the owner of the identity.
13	Information leakage	Information Leakage is an application weakness where an application reveals sensitive data, such as technical details of the web application, environment, or user-specific data. Sensitive data may be used by an attacker to exploit the target web application, its hosting network, or its users.
14	Exploit kits	Exploit kits include a collection of ready-made exploits usually planted in compromised websites or used in malvertising campaigns. Exploit kits have the ability to identify exploitable vulnerabilities in a user's browser or web application and automatically exploit them.
15	Cyber espionage	Cyber espionage describes the stealing of secrets stored in digital formats or on computers and IT networks

ETL is to be treated for indicative purpose and useful to assess the current state-of-play in cyberspace and for cyber defence strategies. Cybersecurity drivers and threats depend on the infrastructure as well as on application, it is essential to understand the vulnerabilities that can effect the current state of cyber infrastructure.

V. CYBERSECURITY IN WEBGIS ENVIRONMENT

Park et al, Rao & Pant and Sankar & Sevugan outlined the issues of Cybersecurity in WebGIS setup [36, 37 and 38]. Park et al concluded that web-based GIS system is open for hackers to be penetrated into port 80 if no dedicated security tools exist and proposed IDS based on Hidden Markov Model (HMM) for securing GIS web servers [36]. If the hacker can corrupt the information stored in GIS system, by hacking into web server which is connected to GIS, it could result in disastrous accidents. Rao & Pant, in their study suggested a holistic framework to study the security and risk assessment of distributed GIS application. They proposed a framework that addresses the security across the three interrelated layers (network layer, host layer, and application). Their study brings forth, a comprehensive model for vulnerability assessment, risk rating for management of Geographical Weather Information System (GWIS) [37]. Sankar & Sevugan proposed hybrid model to deal with information in a secured way that will store and hide the information along with some normalization techniques. Their proposed model results in an efficient way of delivery of information without any loss of data and with minimum time through effective load balancing [38].

The main purpose of WebGIS is to serve the geographic data to the clients. Hence it is essential to secure the information or data that is stored in the WebGIS environment and also it is essential that secure the transit of data [39]. Information security is the process of protecting the availability, privacy, and integrity of data. Risk management is an overall goal of every organization. Information security is one of the disciplines within the organization that addresses risk management [40]. Multiple layers of defence mechanism improve information security.

An Enterprise Web GIS Solution combines the knowledge of complex GIS systems with the standards and best practices of Information Technology to design and implement an end-to-end system that deliver geospatial data services, tools and applications on the web. In order to design an optimal solution that fits well with an enterprise workflow and provide robust, reliable, responsive and scalable map services and applications, it is important to understand the various components of the web GIS framework and consider the key factors that affect them when deciding on the type of technology stack that works best [41]. Cybersecurity implementation depends on the software stack that is being used in the architectural components of a WebGIS system like ESRI ArcGIS Server Architecture, GeoServer or MapServer (Open source software) based architecture, ERDAS Apollo architecture and etc. A typical example of WebGIS stack is postgreSQL/PostGIS as database, GeoServer as a GIS backend, and Openlayers or Leaftlet (Java script library) for web application development [42].

www.cvedetails.com provides an easy to use web interface to Common Vulnerabilities and Exposures (CVE) vulnerability data. Cybersecurity enthusiasts can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them [43]. cve.mitre.org contains a list of entries, each containing an identification number, a description, and at least one public reference for publicly

known Cybersecurity vulnerabilities. These entries are used in numerous Cybersecuirty products and services from around the world, including the U.S National Vulnerability Database (NVD) [44].

Chen et al proposed vulnerability prediction sub-system by using hackers' ad hoc communities and publicly available security sources, the emerging concepts that are the early warning signs of likely vulnerability targets along with mining publicly available vulnerability, exploit, and attack databases like CVEs (cve.mitre.org), CVE Details (cvedetails.com), and OWASP Web Application Security Consortium Web Hacking Incidents Database (WHID) Project to determine prominent concepts. Their mining also includes hacker discussion forums, blogs, and Internet Relay Chat (IRC) channels (e.g. freenode.net, AnonOps IRC, Metasploit IRC, Google ProjectZero, blackhat.com, gmane.org, seclists.org) to identify emerging concepts [45].

During the phases of development and deployment of the web applications it is advisable to check latest vulnerabilities with respect to the version of the software in the stack. Table IV shows the excerpts from the CVE statistics from cvedetails.com and cve.mitre.org for the software in open Geostack (for previous versions of these software).

Table IV. Vulnerable for the software in open Geo-stack

Sl. No.	**Software**	**Vulnerable types (for previous versions)**
1	Postgresql	Denial of Service Code Execution Overflow Multiple stack-based buffer overflow SQL injection Bypass Something and Gain information Multiple format string vulnerabilities CRLF Heap based buffer overflow
2	Mapserver	Denial of Service Execute Code Overflow Directory traversal vulnerability Cross-site scripting
3	Geoserver	Overflow PartialBufferOutputStream2
4	JQuery	Denial of Service Cross-site scripting

Jang-Jaccard & Nepal surveyed the emerging trends in Cybersecurity and published

comprehensive overview of existing security vulnerabilities [46]. Securosis has well documented the security at web application level [47]. With a loose mapping to the Software Development Lifecycle, the security can be divided into three steps as Secure Development, Secure Deployment and Secure Operations as shown in figure 3.

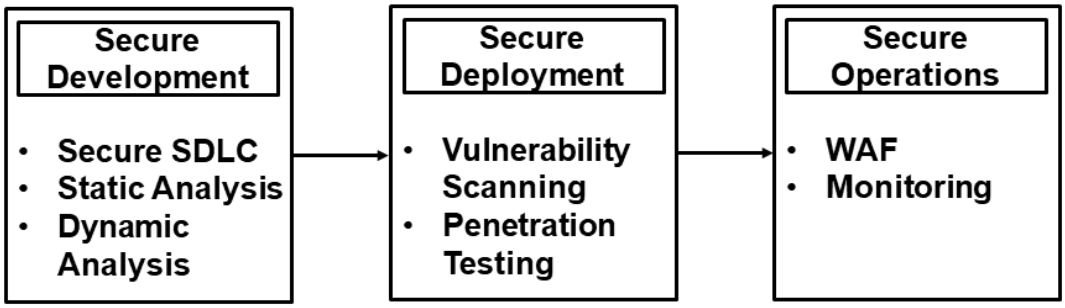

Figure 3. Application Level Security (Adopted from (Securosis, 2009))

Secure Development: This includes training for people who deliver web applications and improved processes to guide their activity. Security awareness training is managed through education and supportive process modifications, as a precursor to making security a functional requirement of the application. Induce secure development practices and software assurance into the web application programming process should be a part of this process. Static analysis aids engineering in identifying vulnerable code using certain tools that scan the source code of an application to look for security errors, often called "white box" tools., and dynamic analysis to detect anomalous application behaviour using tools that interact with a running application and attempt to 'break' it, but don't analyse the source code directly (often called "black box" tools). Fonseca et al in their study submitted the survey results of software development processes to build software products for the web, with security build in. Vulnerabilities like Cross Site Scripting (XSS), SQL Injection, Hidden (but unprotected) content, Cross Site Request Forgery, Debug code, Insecure Object References and Application logic vulnerabilities can be taken care at this stage [48].

Secure Deployment: At the stage where an application is code-complete, or is ready for more rigorous testing and validation, it is time to confirm that it doesn't suffer from serious known security flaws, and is configured such that it is not subject to any known compromises. This is where vulnerability assessments and penetration testing will be done for configuration analysis, threat discovery, patch levels, and operational consistency checking.

- Vulnerability Assessment: Remote scanning of a web application both with and without access credentials to find vulnerabilities. Web application vulnerability assessments focus on the application itself, while standard vulnerability assessments focus on the host platform. May be a product, service, or both.

- Penetration Testing: Penetration testing is the process of actually breaking into an application to determine security vulnerabilities and the risks they pose. While vulnerability assessments find security flaws, penetration tests explore those holes to measure impact and categorize/prioritize. May be a product, service, or both.

Petukhov & Kozlov presented the results of their approach to vulnerability analysis which incorporates advantages of penetration testing and dynamic analysis. Their approach effectively utilizes the extended Tainted Mode model [49].

Secure Operations: Secure operations provide detection capabilities and can react to events from an operational application. The web application firewalls' ability to screen an application from unwanted uses, and monitoring tools that scan requests for inappropriate activity against the application or associated components. Recent developments in detection tools promote enforcement of policies, react intelligently to events, and combine multiple services into a cooperative hybrid model.

- Web Application Firewalls: Network tools that monitor web application traffic and alert on — or attempt to block known attacks.
- Application and Database Activity Monitoring: Tools that monitor application and database activity (via a variety of techniques) for auditing, and generate security alerts based on policy violations.

Web applications are considered the most exposed and least protected, thereafter vulnerable because the standards somehow are not focused on security but more in the serve need functionality [50].

Network security is any activity designed to protect the usability and integrity of network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading the network. Network security combines multiple layers of defences at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors will be blocked from carrying out exploits and threats [51]. Network security paradigms can be classified by either the scope of security measures taken (perimeter, layered) or how proactive the system is [52].

Perimeter Security Approach: In a perimeter security approach, the security efforts will be focused on the perimeter of the network. These include firewalls, proxy servers, password policies and any technology or procedure that makes unauthorized access of the network. In perimeter security approach there is little or no effort is made to secure the systems within the network. Hence the various systems with that perimeter are often vulnerable.

Layered security approach: A layered security approach is one in which not only is the perimeter secured, but individual systems within the network are also secured. Entire infrastructure (servers, network components and etc,.) will be considered and divide the network into segments and secure each segment as if it were a separate network so that, if perimeter security is compromised, not all internal systems are

affected. Layered security is the preferred approach whenever possible. Access control mechanisms, behaviour analytics, firewalls, email security, IDPS, network segmentation, security information and event management, VPN, web security will aid in securing the network.

In WebGIS the most important asset is data. Aerial and Satellite imagery undergoes significant processing before putting into the storage for serving using GIS servers. A strong data storage security process is essential part in chain of WebGIS setup. Data storage security is a broad area that covers everything from legal compliance, through preparedness for e-discovery requests to user access control and the physical security of data storage. Storage security deals with any type of security around the storage architecture and the data stored on it. The security needs of a type of data must reflect the value of that data. Web GIS administrators must ensure that sensitive data is not revealed to a larger audience than intended. Security rules can be applied at various tiers, and may restrict access to end user applications, GIS web services, map layers, geographic features, or feature attributes [53]. When vector data is proprietary or copyright-protected, it may be desirable to show only a rasterized image of map data rather than allow the download of each vertex coordinate. Limits should be placed on the scope of web service requests to avoid web scraping, mass downloads, or enormous data processing jobs that overburden the server (whether intentionally or unintentionally).

Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks. It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment. Database security covers and enforces security on all aspects and components of database which includes data stores in database, database server and database management systems and other database workflow applications [54]. Some of the ways database security is analysed and implemented include:

- Restricting unauthorized access and use by implementing strong and multifactor access and data management controls. PostgreSQL provides a feature called Host Based Authentication (HBA). HBA is a way of explicitly filtering out who can access which database using a specified authentication method. The feature ensures unauthorized access to your PostgreSQL database.
- Load/stress testing and capacity testing of a database to ensure it does not crash in a distributed denial of service (DDoS) attack or user overload
- Physical security of the database server and backup equipment from theft and natural disasters
- Reviewing existing system for any known or unknown vulnerabilities and defining and implementing a road map/plan to mitigate them

Web GIS administrators must work closely with their organization’s existing IT management staff to ensure that web services are secure. For greater administrative control and end-user convenience, web GIS systems and apps should be integrated

with the organization's existing login infrastructure when feasible. Standard web safety practices can boost the security of a GIS, such as granting users only the minimum privileges necessary to do their jobs, restricting physical access to server machines, requiring strong passwords that are changed on a regular basis, and so forth. All passwords and any sensitive spatial or tabular data should be transferred in encrypted form via secure sockets layer (SSL) connections. Any user input allowed into the web GIS should be screened by client and server code for malicious intentions, such as structured query language (SQL) injection attacks [55].

VI. CONCLUSION

In this paper we have reiterated the concepts of WebGIS and explained the need of add-on servers like GIS server to serve the geo-reference data over web. The architecture of WebGIS and the role of networking elements of server side environment were discussed. The uses of uses layer 2 and layer 3 network infrastructures with respect to Cybersecurity have been explained. And finally the vulnerabilities in the WebGIS environment were discussed along with Cybersecurity protective measures. Vulnerabilities and control measures with respect of OSI layers were discussed. The OWASP top 10 vulnerabilities and their importance with respect to Cybersecurity at application level have been appraised. The importance of Cybersecurity ecosystem to combat the vulnerabilities using ENISA Threat Landscape has been elaborated. It has been emphasized that the publicly available security sources like CVE gives the hints about the threats with respect to software stack of WebGIS. By and large the implementation of Cybersecurity in WebGIS environment has been explained by mapping to the software development lifecycle by dividing into secure development, secure deployment and secure operations.

REFERENCES

[1] Von Solms, R., and Van Niekerk, J., 2013, "From information security to cyber security." Computers & security, 38, pp. 97-102.

[2] Dykes, J., 1996, "Dynamic maps for spatial science: a unified approach to cartographic visualization.", Innovations in GIS 3, Parker, D. , eds., Taylor & Franics, London, pp. 177-187.

[3] Parker, H. D., 1988, "The unique qualities of a geographic information system: a commentary." Photogrammetric Engineering and Remote Sensing, 54, pp. 1547-1549.

[4] Burrough, P. A., 1986, "Principles of Geographical Information Systems for Land Resources Assessment." Oxford University Press, New York.

[5] Ozturan, M., Egeli, B., and Bacioglu, F., 2004, "Web-GIS based urban management information system: the case of satellite cities in Istanbul," Management Information Systems, 2004: GIS and Remote Sensing, 8, pp.13-21.

[6] Liu, X., Han, J., Zhong, Y., Han, C., He X., 2009, " Implementing WebGIS on hadoop: A case study of improving small file i/o performance on HDFS." IEEE international conference on cluster computing and workshops, Cluster' 09, pp. 1–8.

[7] Agrawal, S., and Gupta, R. D., 2017, "Web GIS and its architecture: a review." Arabian Journal of Geosciences, 10(23), 518.

[8] Forouzan, A. B., 2006, "Data communications & networking (sie)," Tata McGraw-Hill Education.

[9] Sean-Philip Oriyano., 2016. "CEH v9: Certified Ethical Hacker Version 9 Study Guide." John Wiley & Sons.

[10] Peterson, M. P., 2012. "Online maps with APIs and WebServices,." Springer Science & Business Media.

[11] OGC., 2018, "OGC Standards and Supporting Documents,".

[12] Karnatak, H. C., Saran, S., Bhatia, K., and Roy, P. S., 2007, "Multicriteria spatial decision analysis in web GIS environment." Geoinformatica, 11(4), pp. 407-429.

[13] Rinner, C., and Jankowski, P., 2002, "Web-based spatial decision support-technical foundations and applications," The Encyclopedia of LifeSupport Systems, C. B. Medeiros eds., Advanced Geographic Information Systems, Oxford: UNESCO / Eolss Publishers. pp. 209-234.

[14] Yao, X., and Zou, L., 2008, "Interoperable internet mapping—an open source approach," Cartography and Geographic Information Science, 35(4), pp. 279-293.

[15] Peng, Z. R., 1999, "An assessment framework for the development of Internet GIS," Environment and Planning B: Planning and Design, 26(1), pp. 117-132.

[16] Dragicevic, S., Balram, S., and Lewis, J., 2000, "The role of Web GIS tools in the environmental modeling and decision-making process," 4th International Conference on Integrating GIS and Environmental Modeling (GIS/EM4): Problems, Prospects and Research Needs. Banff, Alberta, Canada, pp. 2-8.

[17] Yang, C. J., Wang, Y. X., Wang, X. L., Dong, P., and Liu, D. L., 2001, "Review of the Main Technologies of WebGIS," J. of Image and Graphics, 9, 012.

[18] Alesheikh, A. A., Helali, H.,and Behroz, H. A., 2002, "Web GIS: technologies and its applications," In Symposium on geospatial theory, processing and applications, 15.

[19] Predic, B., and Stojanovic, D., 2003, "XML Technologies in Web Based Geographic information Systems," Proc. 4th Conference on Informatics and Information Technology, Institute of Informatics, Faculty of Natural Sciences and Mathematics, Ss. Cyril and Methodius University in Skopje, Macedonia,

Skopje, Macedonia, pp. 212-222.

[20] Peng, Z. R., and Tsou, M. H,0. 2003, "Internet GIS: Distributed Geographic Information services for the internet and wireless networks, John Wiley & Sons.

[21] Steiniger, S., and Hunter, A. J., 2012, "Free and open source GIS software for building a spatial data infrastructure," Geospatial free and open source software in the 21st century, pp. 247-261.

[22] Arregoces, M., and Portolani, M., 2003, "Data Center Fundamentals," Cisco Press.

[23] Zimmermann, H., 1980, "OSI reference model--The ISO model of architecture for open systems interconnection, IEEE Transactions on communications, 28(4), pp. 425-432.

[24] Bourke, T., 2001, "Server load balancing," O'Reilly Media Inc.

[25] Tracy, M., Jansen, W., and McLarnon, M., 2002, "Guidelines on Securing Public Web Servers," National Institute of Standards and Technology.

[26] Network Architecture Diagrams, 2018. http://www.uml-diagrams.org/sequence-diagrams. (accessed April 20, 2018).

[27] Surman, G., 2002 "Understanding security using the OSI model," SANS Institute InfoSec Reading Room.

[28] Reed D., 2003, "Applying the OSI seven layer network model to information security," SANS GIAC GSEC Practical Assignment Version 1.4b Option One. SANS Institute.

[29] Meghanathan, N., 2011, "A Tutorial on Network Security: Attacks and Controls," International Journal on Communications Antenna and Propagation (IRECAP), 1(1), pp. 103–116.

[30] Gray, J. D., 2015, "Information Technology Valuation: A Strategy and Risk Based Approach," University of Redlands, InSPIRe @ Redlands.

[31] Finjan, 2016, "Application Layer Security and the OSI Mode."

[32] Kari A. P., 2004, "A Layered Security Model: OSI and Information Security," GIAC Certifications.

[33] OWASP, 2017, "Application Security Risks-2017," Open Web Application Security Project (OWASP).

[34] Curphey M, Endler D, Hau W, Taylor S, Smith T, Russell A, McKenna G, Parke R, McLaughlin K, Tranter N, and Klien A., 2002, "A guide to building secure web applications," The Open Web Application Security Project. 1(1).

[35] ETSI, 2017, "CYBER; Global Cyber Security Ecosystem," ETSI TR 103 306 V1.2.1.

[36] Park, J. S., Jin, H. T., and Kim, D. S., 2004, "Intrusion detection system for

securing geographical information system web servers," Proc. International Workshop on Web and Wireless Geographical Information Systems, Springer, Berlin, Heidelberg, pp. 110-119.

[37] Rao, K. R. M., & Pant, D., 2010, "Security risk assessment of Geospatial Weather Information System (GWIS): An OWASP based approach," International Journal of Computer Science and Information Security, 8(5), pp. 208-218.

[38] Sankar, K., and Sevugan, P., 2016, "An investigation on hybrid computing for competent data storage and secure access for geo-spatial applications," IIOAB journal, 7(5), pp. 139-149.

[39] Rhodes-Ousley, M. 2013, "Information security: the complete reference," McGraw Hill Education.

[40] Information Security, 2018, www.wikigis.com.

[41] Rao, S., and Vinay, S., 2009, "Choosing the Right Frameworks for an Informed Enterprise Web GIS Solution," Center for International Earth Science Information Network.

[42] Mustakayev. R., and Batkayev. S., 2017, "Overview of the stack technology visualization and storing data in developing of Geo-Information system," Proc. 15th International Scientific Conference Information Technologies And Management, ISMA University, Riga, Latvia.

[43] Ozkan, S. 2018., "CVE Details," www.cvedetails.com.

[44] CVE, 2018, "Common Vulnerabilities and Exposures," https://cve.mitre.org

[45] Chen, H. M., Kazman, R., Monarch, I., and Wang, P., 2016, "Predicting and fixing vulnerabilities before they occur: A Big Data Approach," Proc. 2nd International Workshop on BIG Data Software Engineering, ACM, pp. 72-75.

[46] Jang-Jaccard, J., and Nepal, S., 2014, "A survey of emerging threats in Cybersecurity," Journal of Computer and System Sciences, 80(5), pp. 973-993.

[47] Securosis, 2009, "Building a Web Application Security Program," https://securosis.com.

[48] Fonseca, J., Vieira, M., Buragga, K., and Zaman, N., 2013, "A Survey on Secure Software Development Lifecycles," Software Development Techniques for Constructive Information Systems Design, pp. 57-73.

[49] Petukhov, A., and Kozlov, D., 2008, "Detecting security vulnerabilities in web applications using dynamic analysis with penetration testing," Computing Systems Lab, Department of Computer Science, Moscow State University.

[50] Charpentier, R,.J,E., 2013, "Web application Security," http://www.diva-portal.org.

[51] CISCO, 2018, "What Is Network Security?,". https://www.cisco.com.

[52] Easttom II, W. C., 2013, "Network Defence and Countermeasures: Principles and Practices," Pearson IT Certification.

[53] Bertino, E., Thuraisingham, B., Gertz, M., and Damiani, M. L., 2008, "Security and Privacy for Geospatial Data: Concepts and Research Directions," Proc. SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS, New York, pp. 6–19.

[54] Techopedia, 2018, "Database Security," https://www.techopedia.com.

[55] Quinn, S., 2018, "Web GIS. The Geographic Information Science & Technology Body of Knowledge," John P. Wilson (ed).